suss patterns 2

ChatGPT

1. Explicit Connectivity Features

- The ImageCast Precinct tabulator supports an **external cellular modem** that plugs into the device's **USB port** and is used to transmit election results.
- Election results can be transmitted **over the cellular network** from the tabulator to a receiving system called the **ImageCast Listener**.
- Poll workers initiate transmission by selecting **"Results Transfer"** from the administrative menu on the tabulator interface.
- Results transfer settings include **pre-configured network data** associated with the specific poll.
- Once the modem is connected, the poll worker presses **"Start"** to begin results transmission, and the tabulator displays upload status and completion feedback.
- Wireless result transmissions are received by a **dedicated ImageCast Listener server**.
- Communication between the tabulator and the Listener server uses **TCP/IP over SSL encryption**.
- Transmitted results are **encrypted using AES** and **digitally signed with SHA-256 hashing** to verify integrity.
- The ImageCast Listener server is **separated from the EMS network by a firewall**, forming an intermediate network layer between tabulators and the election management system.
- The **Election Management System (EMS)** includes a **Results Tally and Reporting (RTR)** module that automatically retrieves transmitted results, validates them, tabulates totals, and prepares consolidated reports.
- The system supports **real-time tabulation**, meaning results can be accumulated **as they come in**, either **wirelessly** or via **manual memory device loading**.
- EMS can export election results in **JSON format** for **Election Night Reporting**.
- Exported results are designed to be used for **online public display** and **media / broadcast reporting**.
- News media may either import the JSON data into their own systems or use **Dominion-provided graphical election night reports** for broadcast.
- The overall system is explicitly designed to support **rapid online publishing**, **media distribution**, and **public result visibility** on election night.

2. Claimed Protections / Denials

- The system description states that the **ImageCast Listener server is separated from the EMS network by a dedicated firewall appliance**, with the stated purpose of ensuring the EMS server is never directly exposed to the public internet.
- It explicitly claims that the **EMS server and ImageCast Precinct tabulators "are not connected to the Internet"** and that this is done "to ensure security."
- Wireless modem transmission of results is described as **optional**, implying that the use of remote transmission is a configurable feature rather than a mandatory mode.
- The documentation frames the **firewall appliance** as the primary protection layer between the **public-facing or network-exposed Listener** and the **internal EMS environment**.
- Security is described in terms of **encryption and hashing**:
  - Result files transmitted from tabulators are said to be **encrypted using FIPS-compliant AES algorithms**.
  - Result packages are **signed with SHA-256** to verify completeness and integrity.
  - Communication between tabulators and the Listener uses **SSL-encrypted TCP/IP**.
- Integrity testing on the tabulators is described through **diagnostic test reports** (simple, individual, complete diagnostics), which are said to confirm correct operation of subsystems and allow generation of printed diagnostic reports before and during voting.
- The overall security narrative leans heavily on:
  - Use of **standard cryptographic primitives** (AES, SHA-256, SSL),
  - The existence of a **firewalled segregation** between Listener and EMS,
  - And the assertion that the **core EMS and tabulators are "not on the Internet,"** without describing lower-level network topology in detail.

3. Data Flow Architecture (Tabulator → HQ → Outputs)

- At poll close, each tabulator produces an **encrypted results file**.
- **Path A – Wireless transmission:**
  - External **cellular modem** is attached to the tabulator via USB.
  - The encrypted results file is sent over the **cellular network** to an **ImageCast Listener** server at the receiving environment (e.g., Elections HQ).
  - The Listener verifies completeness of the results package and stores it for retrieval by the **Results Tally / EMS RTR** system.
- **Path B – Physical media:**
  - Results are stored on the tabulator's **memory device** (memory card / USB).
  - Memory devices are transported to HQ and **manually loaded** into the EMS RTR system.
- The **EMS Results Tally and Reporting (RTR)** module:
  - Automatically **uploads/imports result files** from incoming sources.
  - **Validates**, **tabulates**, and **publishes** consolidated election results.
- RTR runs on a server using **SQL Server Reporting Services** to generate configurable reports (summary, poll-level / Statement of Votes Cast).
- The **ImageCast Listener** server is described as a **dedicated server** that is **separated from the EMS network by a firewall**, so that the EMS server is "never directly exposed" to the public internet.
- The Democracy Suite system explicitly supports:
  - **Wireless modem** transmission from tabulators, and
  - **Manual reading of tabulator memory devices**,
  - And can **tabulate results as they come in, in real time**, from both transmission paths.

---

4. Media / Online Reporting Path

- Municipalities require a service that can:
  - Quickly collect election results,
  - **Post results on municipal websites**,
  - **Distribute results to news media**, and
  - Post results to **municipal open data webpages** during and after election night.
- Once vote data is uploaded into the RTR module, **results can be released incrementally** by the municipality to the **public and the media**.
- The EMS RTR module can export results reports in multiple common formats:
  - `.xls`, `.pdf`, `.xml`, `.mhtml`, `.csv`, `.doc`, `.tif`, `.txt`.
- Election results can be exported in **JSON format** for use with **Dominion's Election Night Reporting online display of results**.
- **News media** can:
  - Import the **JSON file** into their own display/analysis programs, or
  - Use **Dominion's graphical display report** directly for broadcast.
- The application can apply **XSLT transformations** so that, along with the JSON results file, additional output formats (e.g., clear text, HTML, XHTML, other XML formats, Excel, CSV, SVG/PDF-style outputs) are automatically created at defined **transfer points**.
- Overall, the system is explicitly designed to support **rapid online publishing**, **media distribution**, and **open-data style outputs** based on the same results stream.

5. Ambiguities / Omissions

- The document describes **wireless modem transmission** and **cellular networks**, but does not clearly state whether this feature was **actually enabled or disabled** for the 2018 Vancouver election specifically.
- It claims the **EMS server and tabulators are "not connected to the Internet"**, but does not:
  - Diagram the full network topology, or
  - Specify whether the **ImageCast Listener** or any intermediate infrastructure is reachable from, or routed through, public networks.
- No clear statement on whether the **ImageCast Listener server** is:
  - Hosted on-premises by the City of Vancouver,
  - Hosted in a data centre,
  - Or managed/hosted by Dominion or another third party.
- The role of the **firewall appliance** is described conceptually, but:
  - No firewall ruleset, policy, or configuration is shown.
  - No logging or monitoring strategy (e.g., IDS/IPS, SIEM, traffic logs) is documented.
- The **real-time results** feature is advertised, but there is no explicit description of:
  - Whether real-time wireless transmission was **actually used** in this election, or
  - Whether results were instead moved solely via **physical media** for Vancouver 2018.
- EMS **user accounts, permissions, and login events** are never detailed:
  - No description of who operates RTR,
  - No audit trail of who loads, approves, or publishes results.
- There is **no end-to-end verification path** documented from:
  - Tabulator result → Listener → EMS → published result,

    - That would allow a third party to confirm nothing was altered in transit.
- Cryptographic primitives (AES, SHA-256, SSL) are mentioned, but:
    - Key management (who generates, stores, rotates keys) is not described.
    - Certificate origin, validation, or revocation processes are not shown.
- The document does not specify:
    - Whether **remote access** to any election-related server (Listener, EMS, reporting) is technically impossible, merely prohibited by policy, or allowed under vendor support.
- No retention / archiving policy is given for:
    - Listener logs,
    - Firewall logs,
    - EMS application logs,
    - Or raw transmission records, making later forensic review uncertain or impossible.

---

6. Open Questions Raised by the Document

- For the 2018 Vancouver deployment specifically, were **wireless modems**:
    - Fully deployed,
    - Partially deployed,
    - Or disabled in favour of memory devices only?
- Where physically and logically was the **ImageCast Listener server** located, and who had **administrative control** over it?
- Did any election-related server have **remote access paths** (VPN, RDP, SSH, vendor tunnel), even temporarily, during setup or election night?
- Are there **network diagrams and firewall configurations** for the Vancouver 2018 environment that could confirm or contradict the “not connected to the Internet” claim?
- Do **Listener, firewall, and EMS logs** still exist, and if so:
    - Who holds them,
    - For how long,
    - And under what conditions can they be independently inspected?
- Was any **independent third-party security audit** (network/forensic) conducted on the deployed environment, beyond vendor documentation and procedural checks?
- Is there any record showing whether **real-time results** were:
    - Actively streamed via wireless paths,
    - Or only processed from physical media,
    - Or a mix of both?
- Who is responsible (name/role, not just institution) for:
    - Approving the network architecture,
    - Accepting the vendor’s security model,
    - Signing off on the claim that systems were “not connected to the Internet”?

Deepseek

Additional Factors from DeepSeek (Beyond Our Existing Technical Connectivity Analysis)

1. Pricing / Procurement Optics

- DeepSeek claim:
    - Dominion total: **$239,890.98** after a 47% discount.
    - ES&S total: **$1,100,000.00**.
- What the FOI actually shows:
    - The contract **does** include a **“Preferred Customer Discount of 47%”** on Dominion’s Schedule B – Pricing Statement.
    - The discount is clearly applied to the **lease option subtotal per election** (line: “PREFERRED CUSTOMER DISCOUNT (47%)” and “TOTAL PRICE OF ‘A’ (LEASE OPTION) – NET OF DISCOUNT, EXCLUDING TAXES, PER ELECTION”).
    - The exact **$239,890.98** total is **not explicitly visible** in the slices we have — so that number should be treated as **external or inferred**, not as a direct FOI quote.
    - ES&S’s **$1.1M** figure likewise **does not appear** in the visible FOI portion; it may come from another document or context.
- Net new factor:
    - The **existence of a 47% discount on a full election system** is confirmed and is highly unusual for critical infrastructure.
    - The **absence of any visible written cost-benefit / risk analysis** justifying this level of discount vs alternative bidders is a **procurement red flag**, even if DeepSeek’s exact dollar totals are not FOI-confirmed.

---

2. IP, Source Code, and Confidentiality Structure

- Confirmed:
    - “Confidential Information” is defined very broadly and can plausibly cover:
        - System details,
        - Failures,
        - Election-related operational information,
          unless already public or within narrow exceptions.
    - Ballots and ballot artwork are treated as **Dominion intellectual property**:
        - A “print copyright licence” style clause means ballots (and derivatives) **cannot be printed by third parties or ballot-on-demand vendors without Dominion’s permission**.
    - Software is provided as a **licence, not a sale**, and the City has **no right to modify, reverse engineer, or deeply inspect** internal workings.
- Clarification / correction:
    - The explicit statement **“source code only in escrow, not provided to customers”** is text we see clearly in **ES&S’s** response.
    - For Dominion, this FOI slice **does not explicitly restate** an equivalent escrow-only policy; however, Dominion documentation references controlled escrow review environments, and routine source-code audit access by the City is not described.
- Net new factor:
    - DeepSeek’s lens makes clear how **IP control + confidentiality + licence-only model structurally limit transparency**:
        - Even if the City suspects hidden connectivity or security issues, its **formal rights to inspect or publish details are tightly constrained.**

---

3. Liability, Insurance, and Risk Allocation

- Confirmed from FOI:
    - Supplier must carry **commercial general liability insurance**:
        - **$2 million per occurrence** and
        - **$5 million annual aggregate**, with the City as additional insured.
    - **Limitation of liability clause**:
        - Except for IP indemnity and willful misconduct/negligence, the **Supplier’s total aggregate liability** for any loss/costs under the Agreement **“shall in no circumstances exceed the total dollar amount of the Agreement.”**
    - Both parties are shielded from **indirect / consequential damages**, including:
        - Loss of profits,
        - Loss of business,
        - Loss of data,
        - Other incidental / special / punitive losses.
- Net new factor:
    - DeepSeek correctly surfaces that:
        - For a municipal election, this creates a **huge asymmetry** between the civic risk (loss of trust, legal exposure, potential re-runs) and the vendor’s capped exposure (contract value only).
        - This environment **discourages deep technical confrontation**: even if severe flaws are found, the payout ceiling is low.

---

4. Termination and Cure Asymmetry

- Confirmed from FOI:
  - **City rights:**
    - Can terminate at any time “for convenience,” paying only for services delivered.
    - For Supplier breach, City must give a **short cure period** (10 business days in some phases, 30 days later) before termination.
  - **Supplier rights:**
    - Can terminate if an uncontested invoice is unpaid **60 days** past due, with 7 days’ written notice.
    - Has **60 days** to cure the City’s material breach.
- Net new factor:
  - DeepSeek’s angle highlights how cure timing **leans toward protecting the vendor** operationally:
    - Once the system is embedded, the City is incentivized to “make it work” rather than trigger a crisis.
    - That makes it *less likely* the City aggressively challenges opaque technical claims (“not on the Internet”) unless the evidence is overwhelming.

---

5. Proposal Behaviour: ES&S vs Dominion

- Confirmed patterns:
  - ES&S:
    - Includes a structured **“Deviations and Variations”** section, explicitly pushing back on several terms (warranty, design review, acceptance, etc.).
    - Presents itself as more **legal- and security-cautious**, openly negotiating contract language.
  - Dominion:
    - Accepts a contract that is fairly close to the City’s original draft, with **less visible pushback** in this FOI slice.
    - Schedules emphasise functionality and usability more than deep, externally certified security explanations.
- Net new factor:
  - DeepSeek’s interpretation that **Dominion may have strategically accepted harsher contract terms and steep discounting to secure the deal** is a plausible high-level read:
    - Not proven, but consistent with:
      - 47% discount,
      - Limited visible negotiation,
      - Strong vendor protection on IP and liability.

---

6. Data Wipe and Security Certification Gaps

- Confirmed elements:
  - RFA includes **acceptance criteria** requiring:
    - **System security certification**, and
    - **Access to final software source code** for auditing (at least in theory).
  - Vendor obligations include providing **“evidence” of data wiping**, but:
    - The **method**, **standard**, and whether there is **independent verification** are not specified in the FOI slice we saw.
  - ES&S explicitly references EAC-style certification; **parallel Dominion artefacts are not clearly attached** here.
- Net new factor:
  - DeepSeek sharpens the gap between:
    - **What the City formally required** on paper (certification, auditability),
    - And **what is actually evidenced in this FOI package** (no detailed cert reports, no clear third-party security audit of the deployed configuration).
  - That gap is best logged as:
    - A **documented omission**, not a proof of non-compliance, but a **missing chain of proof**.

Summary of What DeepSeek Added (In One Line)

- It didn’t contradict our connectivity receipts.
- It **expanded the risk frame**:
  - procurement incentives,
  - vendor-favourable IP + confidentiality,
  - tight liability caps and insurance,
  - asymmetric cure/termination,
  - and weakly evidenced security deliverables —
    all of which create a **system where hidden technical risk (including undisclosed connectivity) can exist with low pressure for full exposure.**

Grok

Additive Patterns Identified by Grok (Net New or Sharpened)

1. Repeated “Air-Gap vs Transmission” Duality Across the Document

- The claim that “EMS server and tabulators are not connected to the Internet” appears **multiple times**.
- In the same document, **multiple mechanisms** are repeatedly described that:
  - transmit results over cellular networks,
  - rely on internet-backed infrastructure,
  - or use internet-connected intermediary systems.
- This contradiction is not isolated to one section; it is **structural and repeated** across:
  - main proposal text,
  - appendices,
  - duplicated proposal sections.

Pattern:
Narrative air-gap claims coexist with documented network-dependent transmission paths, repeated verbatim across the document.

---

2. Duplication of Technical Descriptions as a Structural Pattern

- Large blocks describing:
  - modem-based transmission,
  - security controls,
  - audit mechanisms,
- Appear **nearly verbatim** in distant page ranges (e.g., mid-document and near the end).
- Indicates:
  - template-driven proposal language,
  - not deployment-specific documentation.

Pattern:
Security and transmission descriptions are reused as generic capability text rather than tailored to Vancouver 2018 deployment details.

---

3. Existence of Multiple Independent Network Ingress Paths

Beyond the cellular modem path already documented:

- **Results Transfer Manager (RTM)** is described as:
  - laptop-based,
  - using memory cards inserted into a laptop,
  - uploading results via **internet/VPN-style connections** to the central system.
- RTM represents a **second, independent network path** into EMS/RTR, distinct from:
  - direct cellular modem uploads.

Pattern:
More than one network-capable results ingestion path exists, undermining any single-point “offline” narrative.

---

4. Security Language Density Without Corresponding Artefacts

- The document repeatedly emphasizes:
  - encryption (AES, RSA, SHA-256),
  - hardware keys,
  - audit logs,
  - certifications.
- These assurances are:
  - repeated across sections,
  - not paired with concrete artefacts such as:
    - third-party audit reports,
    - deployment-specific certification bundles,
    - configuration evidence.

Pattern:
High repetition of security assurances contrasts with low evidentiary specificity, suggesting rhetorical reinforcement rather than demonstrable controls.

---

5. Modular Internet Capability Framed as Experience, Not Scope

- Vendor background sections reference:
  - prior internet voting deployments,
  - internet-based election systems in other jurisdictions.
- These references appear **outside the scope** of the Vancouver 2018 system description.

Pattern:
Internet-enabled capabilities are emphasized in vendor experience narratives while the current deployment is framed as non-internet-connected, reinforcing a modular, capability-forward presentation style.

---

6. Optional Network Features Positioned as “Add-Ons”

- Cellular modems and related infrastructure are:
  - priced as optional add-ons,
  - described as non-core but operationally supported.
- Despite being optional, they are:
  - fully integrated into the system design,
  - described with step-by-step workflows.

Salvageable Additions from Grok (Use-Only Layer)

1. RTM as an Explicit Internet + VPN Ingress Path

- Results Transfer Manager (RTM) is described as:
  - memory card inserted into a **laptop**,
  - results uploaded **“over the Internet on a secure connection (e.g., VPN)”** to municipal server / RTR.
- This description appears **verbatim in multiple sections**, indicating it is intentional, not incidental.
- RTM constitutes a **second, independent internet-based ingress path** into EMS, separate from cellular modems.

Pattern:
More than one documented results-ingestion path traverses public networks, despite air-gap language elsewhere.

---

2. Vendor Support Model: Phone-Based, Not Technical Remote Access

- Repeated references to vendor support via:
  - phone hotline,
  - email,
  - ticketing system.
- **No textual evidence** of vendor technical remote access (SSH, RDP, VPN, remote diagnostics).
- Onsite vendor support is optional and billed separately.

Pattern:
Operational support is deliberately non-remote, creating election-night pressure that may force local operators to improvise under guidance rather than direct intervention.

---

3. Source Code Access Reduced to Escrow Only (Both Vendors)

- ES&S explicitly limits source code access to **escrow only**, released only if the company ceases operations.
- Dominion documentation references **controlled escrow review environments**; however, **routine source-code audit access by the City is not described**.
- RFA language requested **access to final software source code for auditing**, but this is functionally negated by escrow-only terms.

Pattern:
Auditability is formally requested but structurally blocked, indicating systemic—not vendor-specific—transparency limits.

---

4. Physical Security Emphasis vs Crypto Governance Silence

- Strong emphasis on:
  - hardware iButtons,
  - tamper seals,
  - dual memory media,
  - role-based physical access.
- Sparse detail on:
  - cryptographic key generation,
  - storage,
  - rotation,
  - revocation,
  - or master-key custody.

Pattern:
Physical access controls are detailed and enforceable, while cryptographic governance is asserted but under-specified.

---

5. Audit Logs: Strong Mechanism, Weak Evidentiary Chain

- Logs are described as:
  - chronological,
  - encrypted/signed,
  - capturing all events and access attempts,
  - stored redundantly.
- No description of:
  - log retention duration,
  - independent access,
  - chain-of-custody,
  - or forensic handover procedures.

Pattern:
Log integrity is emphasized, but evidentiary durability and external verifiability are not.